UNITED STATES DISTRICT COURT
FOR THE WESTERN DISTRICT OF NORTH CAROLINA

PRISCILLA UNDERWOOD, individually and on behalf of all others similarly situated, Plaintiff, v. THE CHARLOTTE-MECKLENBURG HOSPITAL AUTHORITY (d/b/a ATRIUM HEALTH), Defendant.	Case No. 3:24-cv-858 **COMPLAINT – CLASS ACTION** **JURY TRIAL DEMANDED**

Plaintiff Priscilla Underwood ("Plaintiff") individually and on behalf of all others similarly situated, by and through her undersigned counsel, brings this Class Action Complaint against The Charlotte-Mecklenburg Hospital Authority (d/b/a Atrium Health) ("Atrium Health" or "Defendant"). Plaintiff alleges the following upon information and belief based on and the investigation of counsel, except as to those allegations that specifically pertain to Plaintiff, which are alleged upon personal knowledge.

INTRODUCTION

1. Plaintiff and the proposed Class Members bring this class action lawsuit on behalf of all persons who entrusted Atrium Health with sensitive personally identifiable information ("PII")[1] and protected health information ("PHI", and collectively with PII, "Private Information") that was impacted in a data breach (the "Data Breach" or the "Breach").

2. Plaintiff's claims arise from Defendant's failure to properly secure and safeguard Private Information that was entrusted to it, and its accompanying responsibility to store and transfer that information.

[1] Personally identifiable information generally incorporates information that can be used to distinguish or trace an individual's identity, either alone or when combined with other personal or identifying information. 2 C.F.R. § 200.79. At a minimum, it includes all information that on its face expressly identifies an individual.

3. Atrium Health is a healthcare provider that operates 40 hospitals, 7 freestanding emergency departments, over 30 urgent care centers, and more than 1,400 care locations North Carolina, South Carolina, Georgia, and Alabama.[2]

4. Defendant had numerous statutory, regulatory, contractual, and common law duties and obligations, including those based on their affirmative representations to Plaintiff and Class Members, to keep their Private Information confidential, safe, secure, and protected from unauthorized disclosure or access.

5. On April 29, 2024, Atrium Health discovered that an unauthorized third party gained access to its IT network.[3]

6. Atrium Health immediately began an investigation to determine the nature and scope of the Data Breach.[4] The investigation determined that the unauthorized third party had access to Atrium Health's IT network between April 29, 2024 and April 30, 2024.[5]

7. On September 13, 2024, Atrium Health issued a public notice of the Data Breach, and began notifying individuals whose Private Information was compromised.[6]

8. Atrium Health indicated that the Private Information impacted by the Data Breach may have included "an individual's first and/or last name; middle initial; street address, email address and/or phone number(s); Social Security number; date of birth; medical record number; certain government or employer identifiers; driver's license or state-issued identification number; bank or financial account numbers or information, including routing numbers, financial institution name, or expiration date; treatment/diagnosis, provider name, prescription, health insurance or

[2] ATRIUM HEALTH, https://atriumhealth.org/ (last visited September 23, 2024).
[3] *Phishing Email May Have Impacted Personal Information*, ATRIUM HEALTH (Sept. 13, 2024), https://atriumhealth.org/about-us/newsroom/news/phishing-email-may-have-impacted-personal-information (last visited September 23, 2024).
[4] *Id.*
[5] *Id.*
[6] *Id.*

treatment cost information; patient identification number; health insurance account or policy number(s); incidental health references; billing identification numbers; access credentials; and/or digital signatures."[7]

9. Defendant failed to take precautions designed to keep its patients' Private Information secure, such as training personnel to detect and prevent phishing attempts, encrypting the information, or deleting the information when it is no longer needed.

10. Defendant owed Plaintiff and Class Members a duty to take all reasonable and necessary measures to keep the Private Information it collected safe and secure from unauthorized access. Defendant solicited, collected, used, and derived a benefit from the Private Information, yet breached its duty by failing to implement or maintain adequate security practices.

11. Defendant admits that information in its system was accessed by unauthorized individuals through a phishing attack on several employee email accounts.

12. The sensitive nature of the data exposed through the Data Breach signifies that Plaintiff and Class Members have suffered irreparable harm. Plaintiff and Class Members have lost the ability to control their private information and are subject to an increased risk of identity theft.

13. Defendant, despite having the financial wherewithal and personnel necessary to prevent the Data Breach, nevertheless failed to use reasonable security procedures and practices appropriate to the nature of the sensitive, unencrypted information it maintained for Plaintiff and Class Members, causing the exposure of Plaintiff's and Class Members' Private Information.

[7] See *Atrium Health, A Notice to our Patients*, ATRIUM HEALTH, https://cdn.atriumhealth.org/-/media/documents/substitute-notices/atrium-health--charlotte-bec--substitute-notice-final.pdf?rev=c6bed3cc96eb4694b4a578c73fd0fca1&hash=58A4D4F600E2F7C506933E7A53B (last visited September 23, 2024).

14. As a result of Defendant's inadequate digital security and notice process, Plaintiff and Class Members' Private Information was exposed to criminals. Plaintiff and the Class Members have suffered and will continue to suffer injuries including: financial losses caused by misuse of their Private Information; the loss or diminished value of their Private Information as a result of the Data Breach; lost time associated with detecting and preventing identity theft; and theft of personal and financial information.

15. Moreover, as an ongoing harm resulting from the Data Breach, Plaintiff and Class Members experienced disruptions in services because Defendant's network systems were offline and inaccessible to patients. These disruptions included delays in obtaining prescription medications, inability to access patient health records via Defendant's online patient portal, cancellation of medical appointments with providers, and inability to schedule medical appointments.

16. Plaintiff brings this action on behalf of all persons whose Private Information was compromised as a result of Defendant's failure to: (i) adequately protect the Private Information of Plaintiff and Class Members; (ii) warn Plaintiff and Class Members of Defendant's inadequate information security practices; (iii) effectively secure hardware containing protected Private Information using reasonable and adequate security procedures free of vulnerabilities and incidents; and (iv) timely notify Plaintiff and Class Members of the Data Breach. Defendant's conduct amounts to at least negligence and violates federal and state statutes.

17. Plaintiff brings this action individually and on behalf of a Nationwide Class of similarly situated individuals against Defendant for: negligence; negligence per se; unjust enrichment, breach of implied covenant of good faith and fair dealing, and invasion of confidence.

18. Plaintiff seeks to remedy these harms and prevent any future data compromise on behalf of themselves and all similarly situated persons whose personal data was compromised and

stolen as a result of the Data Breach and who remain at risk due to Defendant's inadequate data security practices.

PARTIES

Plaintiff

19. Plaintiff Priscilla Underwood is a resident of York, South Carolina. Plaintiff is a patient of Atrium Health. As a result of the Data Breach, Plaintiff has experienced an uptick in spam calls and messages. As a consequence of the Data Breach, Plaintiff has been forced to, and will continue to, invest significant time monitoring her accounts to detect and reduce the consequences of likely identity fraud. As a result of the Data Breach, Plaintiff is now subject to substantial and imminent risk of future harm. Plaintiff would not have used Defendant's services had she known that it would expose her sensitive Private Information.

Defendant

20. Defendant The Charlotte-Mecklenburg Hospital Authority (d/b/a Atrium Health) is a healthcare system with headquarters located at Carolinas Medical Center, 1000 Blythe Blvd., Charlotte, North Carolina 28203.

JURISDICTION AND VENUE

21. This Court has jurisdiction over this action under the Class Action Fairness Act, 28 U.S.C. § 1332(d)(2). The amount in controversy exceeds $5 million, exclusive of interest and costs. At least one member of the Class defined below is a citizen of a different state than Defendant, and there are more than 100 putative Class Members.

22. This Court has personal jurisdiction over Defendant because Defendant is registered to do business, and maintains its principal place of business, in Charlotte, North Carolina.

23. Venue is proper in this District under 28 U.S.C. § 1391(b)(2) because Defendant is headquartered in this District, and a substantial part of the events or omissions giving rise to Plaintiff's claims occurred in this District.

FACTUAL ALLEGATIONS

A. Background on Defendant

24. Atrium Health is a healthcare provider that operates 40 hospitals, 7 freestanding emergency departments, over 30 urgent care centers, and more than 1,400 care locations North Carolina, South Carolina, Georgia, and Alabama.[8]

25. In the ordinary course of its business practices, Defendant stores, maintains, and uses an individuals' Private Information.

26. Upon information and belief, Defendant made promises and representations to its patients, including Plaintiff and Class Members, that the Private Information collected from them would be kept safe and confidential, and that the privacy of that information would be maintained.

27. Plaintiff and Class Members provided their Private Information to Defendant with the reasonable expectation and on the mutual understanding that Defendant would comply with its obligations to keep such information confidential and secure from unauthorized access.

28. As a result of collecting and storing the Private Information of Plaintiff and Class Members for its own financial benefit, Defendant had a continuous duty to adopt and employ reasonable measures to protect Plaintiff and the Class Members' Private Information from disclosure to third parties.

B. The Data Breach

29. On April 29, 2024, Atrium Health discovered that an unauthorized third party

[8] ATRIUM HEALTH, https://atriumhealth.org/ (last visited September 23, 2024).

gained access to its IT network.[9]

30. Atrium Health immediately began an investigation to determine the nature and scope of the Data Breach.[10] The investigation determined that the unauthorized third party had access to Atrium Health's IT network between April 29, 2024 and April 30, 2024.[11]

31.

32. On September 13, 2024, Atrium Health issued a public notice of the Data Breach, and began notifying individuals whose Private Information was compromised.[14]

33.

34. Plaintiff's claims arise from Defendant's failure to safeguard their Private Information and failure to provide timely notice of the Data Breach.

35. Defendant failed to take precautions designed to keep its patients' Private Information secure.

36. While Defendant sought to minimize the damage caused by the Data Breach, it cannot and has not denied that there was unauthorized access to the sensitive Private Information of Plaintiff and Class Members.

37. Individuals affected by the Data Breach are, and remain, at risk that their data will be sold or listed on the dark web and, ultimately, illegally used in the future.

C. Defendant's Failure to Prevent, Identify, and Timely Report the Data Breach

38. Defendant admits that unauthorized third persons accessed its network systems.

---

[9] *Phishing Email May Have Impacted Personal Information*, ATRIUM HEALTH (Sept. 13, 2024), https://atriumhealth.org/about-us/newsroom/news/phishing-email-may-have-impacted-personal-information (last visited September 23, 2024).
[10] *Id.*
[11] *Id.*
[13] *Id.*
[14] *Id.*
[17] See *Atrium Health, A Notice to our Patients*, Atrium Health, https://cdn.atriumhealth.org/-/media/documents/substitute-notices/atrium-health--charlotte-bec--substitute-notice-final.pdf?rev=c6bed3cc96eb4694b4a578c73fd0fca1&hash=58A4D4F600E2F7C506933E7A53B (last visited September 23, 2024).

39. Defendant failed to take adequate measures to protect its computer systems against unauthorized access.

40. The Private Information that Defendant allowed to be exposed in the Data Breach is the type of private information that Defendant knew or should have known would be the target of cyberattacks.

41. Despite its own knowledge of the inherent risks of cyberattacks, and notwithstanding the FTC's data security principles and practices,[18] Defendant failed to disclose that its systems and security practices were inadequate to reasonably safeguard its past and present patients' sensitive Private Information.

42. The FTC directs businesses to use an intrusion detection system to expose a breach as soon as it occurs, monitor activity for attempted hacks, and have an immediate response plan if a breach occurs.[19] Immediate notification of a Data Breach is critical so that those impacted can take measures to protect themselves.

43. Despite this guidance, Defendant waited several months after being made aware of the Data Breach to issue a public notice.

D. Data Breaches Cause Disruptions That Put Patients at an Increased Risk of Harm

44. Cyber-attacks at medical facilities, such as Defendant's, are especially problematic because of the disruption they cause to the health treatment and overall daily lives of patients affected by the attack.

45. For instance, loss of access to patient histories, charts, images, and other information forces providers to limit or cancel patient treatment due to a disruption of service. This

[18] *Protecting Personal Information: A Guide for Business,* FED. TRADE COMM'N (Oct. 2016), https://www.ftc.gov/business-guidance/resources/protecting-personal-information-guide-business (last visited September 23, 2024).
[19] *Id.*

leads to a deterioration in the quality of overall care patients receive at facilities affected by cyber-attacks and related data breaches.

46. Research has found that at medical facilities that experience a data breach, the incident increases the risk of complications, affects patient outcomes, and causes an increase in patient mortality rates.[20]

47. Similarly, cyber-attacks and related data security incidents inconvenience patients in a variety of ways, including, but not limited to, the following:

a. rescheduling of medical treatment;

b. being forced to find alternative medical care and treatment;

c. delays or outright cancellation of medical care and treatment;

d. undergoing medical care and treatment without medical providers having access to a complete medical history and records; and

e. the indefinite loss of personal medical history.

E. The Harm Caused by the Data Breach Now and Going Forward

48. Victims of data breaches are susceptible to becoming victims of identity theft. The FTC defines identity theft as "a fraud committed or attempted using the identifying information of another person without authority." 17 C.F.R. § 248.201(9). When "identity thieves have your personal information, they can drain your bank account, run up charges on your credit cards, open new utility accounts, or get medical treatment on your health insurance."[21]

49. The type of data that may have been accessed and compromised here – such as, full names and Social Security numbers – can be used to perpetrate fraud and identity theft. Social

[20] Steve Alder, *66% of Healthcare Organizations Say Patient Care was Disrupted by a Cyberattack*, THE HIPAA JOURNAL. (Oct. 12, 2023), https://www.hipaajournal.com/66pc-healthcare-organizations-patient-care-disruption-cyberattack/#:~:text=Healthcare%20organizations%20are%20having%20to,increase%20in%20patient%20mortality%20rates (last visited September 23, 2024).

[21] *Prevention and Preparedness*, NEW YORK STATE POLICE, https://troopers.ny.gov/prevention-and-preparedness (last visited September 23, 2024).

Security numbers are widely regarded as the most sensitive information hackers can access. Social Security numbers and dates of birth together constitute high risk data.

50. Plaintiff and Class Members face a substantial risk of identity theft given that their Social Security numbers, addresses, dates of birth, and other important Private Information were compromised in the Data Breach. Once a Social Security number is stolen, it can be used to identify victims and target them in fraudulent schemes and identity theft.

51. Stolen Private Information is often trafficked on the "dark web," a heavily encrypted part of the Internet that is not accessible via traditional search engines. Law enforcement has difficulty policing the "dark web" due to this encryption, which allows users and criminals to conceal their identities and online activity.

52. When malicious actors infiltrate companies and copy and exfiltrate the Private Information that those companies store, the stolen information often ends up on the dark web where malicious actors buy and sell that information for profit.[22]

53. For example, when the U.S. Department of Justice announced their seizure of AlphaBay—the largest online "dark market"—in 2017, AlphaBay had more than 350,000 listings, many of which concerned stolen or fraudulent documents that could be used to assume another person's identity."[23] Marketplaces similar to the now-defunct AlphaBay continue to be "awash with [PII] belonging to victims from countries all over the world."[24] As data breaches continue to reveal, "PII about employees, customers and the public are housed in all kinds of organizations,

[22] *Shining a Light on the Dark Web with Identity Monitoring*, IDENTITYFORCE (Dec. 28, 2020) https://www.identityforce.com/blog/shining-light-dark-web-identity-monitoring (last visited September 23, 2024)..
[23] *Stolen PII & Ramifications: Identity Theft and Fraud on the Dark Web*, ARMOR (April 3, 2018), https://res.armor.com/resources/blog/stolen-pii-ramifications-identity-theft-fraud-dark-web/ (last visited September 23, 2024)..
[24] *Id.*

and the increasing digital transformation of today's businesses only broadens the number of potential sources for hackers to target."[25]

54. PII remains of high value to criminals, as evidenced by the prices they will pay through the dark web. Numerous sources cite dark web pricing for stolen identity credentials. For example, personal information can be sold at a price ranging from $40 to $200, and bank details have a price range of $50 to $200.[26] Criminals can also purchase access to entire company data breaches from $900 to $4,500.[27]

55. A compromised or stolen Social Security number cannot be addressed as simply as a stolen credit card. An individual cannot obtain a new Social Security number without significant work. Preventive action to defend against the possibility of misuse of a Social Security number is not permitted; rather, an individual must show evidence of actual, ongoing fraud activity to obtain a new number. Even then, however, obtaining a new Social Security number may not suffice. According to Julie Ferguson of the Identity Theft Resource Center, "The credit bureaus and banks are able to link the new number very quickly to the old number, so all of that old bad information is quickly inherited into the new Social Security number."[28]

56. The Private Information compromised in the Data Breach demands a much higher price on the black market. Martin Walter, senior director of the cybersecurity firm RedSeal, explained: "Compared to credit card information, personally identifiable information and Social Security numbers are worth more than 10 times on the black market."[29]

---

[25] *Id.*
[26] *Id.*
[27] Bryan Naylor, *Victims of Social Security Number Theft Find It's Hard to Bounce Back*, NPR (Feb. 9, 2015) https://www.npr.org/2015/02/09/384875839/data-stolen-by-anthem-s-hackers-has-millions-worrying-about-identity-theft (last visited September 23, 2024)..
[28] *Id.*
[29] *Experts advise compliance not same as security*, RELIAS MEDIA (Mar. 1, 2015) https://www.reliasmedia.com/articles/134827-experts-advise-compliance-not-same-as-security (last visited September 23, 2024). .

57. According to the FBI's Internet Crime Complaint Center (IC3) 2019 Internet Crime Report, Internet-enabled crimes reached their highest number of complaints and dollar losses in 2019, resulting in more than $3.5 billion in losses to individuals and business victims.[30]

58. Further, according to the same report, "rapid reporting can help law enforcement stop fraudulent transactions before a victim loses the money for good."[31] Defendant did not rapidly report to Plaintiff and Class Members that their Private Information had been stolen. Defendant notified impacted individuals five months after learning of the Breach.

59. As a result of the Data Breach, the Private Information of Plaintiff and Class Members has been exposed to criminals for misuse. The injuries suffered by Plaintiff and Class Members, or likely to be suffered as a direct result of Defendant's Data Breach, include: (a) theft of their Private Information; (b) costs associated with the detection and prevention of identity theft; (c) costs associated with time spent and the loss of productivity from taking time to address and attempt to ameliorate, mitigate, and deal with the consequences of this Breach; (d) invasion of privacy; (e) the emotional distress, stress, nuisance, and annoyance of responding to, and resulting from, the Data Breach; (f) the actual and/or imminent injury arising from actual and/or potential fraud and identity theft resulting from their personal data being placed in the hands of the ill-intentioned hackers and/or criminals; (g) damage to and diminution in value of their personal data entrusted to Defendant with the mutual understanding that Defendant would safeguard their Private Information against theft and not allow access to and misuse of their personal data by any unauthorized third party; and (h) the continued risk to their Private Information, which remains in the possession of Defendant, and which is subject to further injurious breaches so long as

[30] *2019 Internet Crime Report Released*, FBI (Feb. 11, 2020) https://www.fbi.gov/news/stories/2019-internet-crime-report-released-021120#:~:text=IC3%20received%20467%2C361%20complaints%20in,%2Ddelivery%20scams%2C%20and%20extortion (last visited September 23, 2024)..
[31] *Id.*

Defendant fails to undertake appropriate and adequate measures to protect Plaintiff and Class Members' Private Information.

60. In addition to a remedy for economic harm, Plaintiff and Class Members maintain an interest in ensuring that their Private Information is secure, remains secure, and is not subject to further misappropriation and theft.

61. Defendant disregarded the rights of Plaintiff and Class Members by (a) intentionally, willfully, recklessly, or negligently failing to take adequate and reasonable measures to ensure that its network servers were protected against unauthorized intrusions; (b) failing to disclose that it did not have adequately robust security protocols and training practices in place to safeguard Plaintiff and Class Members' Private Information; (c) failing to take standard and reasonably available steps to prevent the Data Breach; (d) concealing the existence and extent of the Data Breach for an unreasonable duration of time; and (e) failing to provide Plaintiff and Class Members prompt and accurate notice of the Data Breach.

62. The actual and adverse effects to Plaintiff and Class Members, including the imminent, immediate, and continuing increased risk of harm for identity theft, identity fraud and/or medical fraud directly or proximately caused by Defendant's wrongful actions and/or inaction and the resulting Data Breach require Plaintiff and Class Members to take affirmative acts to recover their peace of mind and personal security including, without limitation, purchasing credit reporting services, purchasing credit monitoring and/or internet monitoring services, frequently obtaining, purchasing and reviewing credit reports, bank statements, and other similar information, instituting and/or removing credit freezes and/or closing or modifying financial accounts, for which there is a financial and temporal cost. Plaintiff and other Class Members have suffered, and will continue to suffer, such damages for the foreseeable future.

CLASS ALLEGATIONS

63. Plaintiff brings this action pursuant to Rule 23 of the Federal Rules of Civil Procedure, individually and on behalf of the following Nationwide Class:

> All persons in the United States who were impacted by the Data Breach publicly announced by Defendant in September of 2024 (the "Class").

64. Specifically excluded from the Class are Defendant, its officers, directors, agents, trustees, parents, children, corporations, trusts, representatives, employees, principals, servants, partners, joint venturers, or entities controlled by Defendant, and its heirs, successors, assigns, or other persons or entities related to or affiliated with Defendant and/or its officers and/or directors, the judge assigned to this action, and any member of the judge's immediate family.

65. Plaintiff reserves the right to amend the Class definitions above if further investigation and/or discovery reveals that the Class should be expanded, narrowed, divided into subclasses, or otherwise modified in any way.

66. This action may be certified as a class action under Federal Rule of Civil Procedure 23 because it satisfies the numerosity, commonality, typicality, adequacy, and superiority requirements therein.

67. Numerosity (Rule 23(a)(1)): The Class is so numerous that joinder of all Class Members is impracticable. Although the precise number of such persons is unknown, and the facts are presently within the sole knowledge of Defendant, upon information and belief, Plaintiff estimates that the Class is comprised of thousands of Class Members, if not more. The Class is sufficiently numerous to warrant certification.

68. Typicality of Claims (Rule 23(a)(3)): Plaintiff's claims are typical of those of other Class Members because Plaintiff, like the unnamed Class, had her Private Information compromised as a result of the Data Breach. Plaintiff is a member of the Class, and her claims

are typical of the claims of the members of the Class. The harm suffered by Plaintiff is similar to that suffered by all other Class Members which was caused by the same misconduct by Defendant.

69. Adequacy of Representation (Rule 23(a)(4)): Plaintiff will fairly and adequately represent and protect the interests of the Class. Plaintiff has no interests antagonistic to, nor in conflict with, the Class. Plaintiff has retained competent counsel who are experienced in consumer and commercial class action litigation and who will prosecute this action vigorously.

70. Superiority (Rule 23(b)(3)): A class action is superior to other available methods for the fair and efficient adjudication of this controversy. Because the monetary damages suffered by individual Class Members are relatively small, the expense and burden of individual litigation make it impossible for individual Class Members to seek redress for the wrongful conduct asserted herein. If Class treatment of these claims is not available, Defendant will likely continue its wrongful conduct, will unjustly retain improperly obtained revenues, or will otherwise escape liability for its wrongdoing as asserted herein.

71. Predominant Common Questions (Rule 23(a)(2)): The claims of all Class Members present common questions of law or fact, which predominate over any questions affecting only individual Class Members, including:

a. Whether Defendant failed to implement and maintain reasonable security procedures and practices appropriate to the nature and scope of the information compromised in the Data Breach;

b. Whether Defendant's data security systems prior to and during the Data Breach complied with applicable data security laws and regulations;

c. Whether Defendant's storage of Class Member's Private Information was done in a negligent manner;

d. Whether Defendant had a duty to protect and safeguard Plaintiff and Class Members' Private Information;

e. Whether Defendant's conduct was negligent;

f. Whether Defendant's conduct violated Plaintiff and Class Members' privacy;

g. Whether Defendant took sufficient steps to secure its customers' Private Information;

h. Whether Defendant was unjustly enriched; and

i. The nature of relief, including damages and equitable relief, to which Plaintiff and Class Members are entitled.

72. Information concerning Defendant's policies is available from Defendant's records.

73. Plaintiff knows of no difficulty which will be encountered in the management of this litigation which would preclude its maintenance as a class action.

74. The prosecution of separate actions by individual members of the Class would run the risk of inconsistent or varying adjudications and establish incompatible standards of conduct for Defendant. Prosecution as a class action will eliminate the possibility of repetitious and inefficient litigation.

75. Defendant has acted or refused to act on grounds generally applicable to the Class, thereby making appropriate final injunctive relief or corresponding declaratory relief with respect to the Class as a whole.

76. Given that Defendant had not indicated any changes to its conduct or security measures, monetary damages are insufficient and there is no complete and adequate remedy at law.

CAUSES OF ACTION

COUNT I
NEGLIGENCE
(On Behalf of Plaintiff and All Class Members)

77. Plaintiff incorporates by reference and re-alleges each and every allegation set forth above in paragraphs 1 through 18 and paragraphs 24 through 62 as though fully set forth herein.

78. Plaintiff brings this claim individually and on behalf of the Class Members.

79. Defendant knowingly collected, came into possession of, and maintained Plaintiff and Class Members' Private Information, and had a duty to exercise reasonable care in safeguarding, securing, and protecting such information from being compromised, lost, stolen, misused, and/or disclosed to unauthorized parties.

80. Defendant had a duty to have procedures in place to detect and prevent the loss or unauthorized dissemination of Plaintiff and Class Members' Private Information.

81. Defendant had, and continues to have, a duty to timely disclose that Plaintiff's and Class Members' Private Information within its possession was compromised and precisely the types of information that were compromised.

82. Defendant owed a duty of care to Plaintiff and Class Members to provide data security consistent with industry standards, applicable standards of care from statutory authority like Section 5 of the FTC Act, and other requirements discussed herein, and to ensure that its systems and networks, and the personnel responsible for them, adequately protected its patients' Private Information.

83. Defendant's duty of care to use reasonable security measures arose as a result of the special relationship that existed between Defendant and its patients. Defendant was in a position to ensure that its systems were sufficient to protect against the foreseeable risk of harm to Plaintiff and Class Members from a data breach.

84. Defendant's duty to use reasonable care in protecting confidential data arose not only as a result of the statutes and regulations described above, but also because Defendant is bound by industry standards to protect confidential Private Information.

85. Defendant breached these duties by failing to exercise reasonable care in safeguarding and protecting Plaintiff and Class Members' Private Information.

86. The specific negligent acts and omissions committed by Defendant include, but are not limited to, the following:

a. Failing to adopt, implement, and maintain adequate security measures to safeguard Plaintiff and Class Members' Private Information;

b. Failing to adequately monitor the security of its networks and systems; and

c. Failing to periodically ensure that its computer systems and networks had plans in place to maintain reasonable data security safeguards.

87. Defendant, through its actions and/or omissions, unlawfully breached its duties to Plaintiff and Class Members by failing to exercise reasonable care in protecting and safeguarding Plaintiff and Class Members' Private Information within Defendant's possession.

88. Defendant, through its actions and/or omissions, unlawfully breached its duties to Plaintiff and Class Members by failing to have appropriate procedures in place to detect and prevent dissemination of Plaintiff's and Class Members' Private Information.

89. Defendant, through its actions and/or omissions, unlawfully breached its duty to timely disclose to Plaintiff and Class Members that the Private Information within Defendant's possession might have been compromised and precisely the type of information compromised.

90. Defendant breached the duties set forth in 15 U.S.C. § 45, the FTC guidelines, the National Institute of Standards and Technology's Framework for Improving Critical Infrastructure Cybersecurity, and other industry guidelines. In violation of 15 U.S.C. § 45, Defendant failed to implement proper data security procedures to adequately and reasonably protect Plaintiff's and Class Members' Private Information. In violation of the FTC guidelines, *inter alia,* Defendant did not protect the personal patient information it keeps; failed to properly dispose of personal information that was no longer needed; failed to encrypt information stored on computer networks; lacked the requisite understanding of its networks' vulnerabilities; and failed to implement policies to correct security issues.

91. Defendant's failure to comply with applicable laws and regulations constitutes negligence *per se*.

92. It was foreseeable that Defendant's failure to use reasonable measures to protect Plaintiff and Class Members' Private Information would result in injury to Plaintiff and Class Members. Further, the breach of security was reasonably foreseeable given the known high frequency of cyberattacks and data breaches.

93. It was foreseeable that the failure to adequately safeguard Plaintiff and Class Members' Private Information would result in injuries to Plaintiff and Class Members.

94. Defendant's breach of duties owed to Plaintiff and Class Members caused Plaintiff and Class Members' Private Information to be compromised.

95. But for Defendant's negligent conduct and breach of the above-described duties owed to Plaintiff and Class Members, their Private Information would not have been compromised.

96. As a result of Defendant's failure to timely notify Plaintiff and Class Members that their Private Information had been compromised, Plaintiff and Class Members are unable to take the necessary precautions to mitigate damages by preventing future fraud.

97. As a result of Defendant's negligence and breach of duties, Plaintiff and Class Members are in danger of imminent harm in that their Private Information, which is still in the possession of third parties, will be used for fraudulent purposes, and Plaintiff and Class Members have and will suffer damages including: a substantial increase in the likelihood of identity theft; the compromise, publication, and theft of their personal information; loss of time and costs associated with the prevention, detection, and recovery from unauthorized use of their personal information; the continued risk to their personal information; future costs in terms of time, effort, and money that will be required to prevent, detect, and repair the impact of the personal

information compromised as a result of the Data Breach; and overpayment for the services or products that were received without adequate data security.

COUNT II
NEGLIGENCE *PER SE*
(On Behalf of Plaintiff and All Class Members)

98. Plaintiff incorporates by reference and re-alleges each and every allegation set forth above in paragraphs 1 through 18 and paragraphs 24 through 62 as though fully set forth herein.

99. Section 5 of the FTC Act, 15 U.S.C. 45, prohibits "unfair . . . practices in or affecting commerce" including, as interpreted and enforced by the FTC, the unfair act or practice by Defendant of failing to use reasonable measures to protect Plaintiff and Class members' Private Information. Various FTC publications and orders also form the basis of Defendant's duty.

100. Defendant violated Section 5 of the FTC Act (and similar state statutes) by failing to use reasonable measures to protect Plaintiff and Class members' Private Information and by failing to comply with industry standards.

101. Defendant's conduct was particularly unreasonable given the nature and amount of Private Information obtained and stored and the foreseeable consequences of a data breach on Defendant's systems.

102. Class Members are consumers within the class of persons Section 5 of the FTC Act (and similar state statutes) were intended to protect.

103. Moreover, the harm that has occurred is the type of harm the FTC Act (and similar state statutes) was intended to guard against. Indeed, the FTC has pursued over fifty enforcement actions against businesses which, as a result of their failure to employ reasonable data security measures and avoid unfair and deceptive practices, caused the same harm suffered by Plaintiff and Class Members.

104. As a result of Defendant's negligence, Plaintiff and Class Members have been

harmed and have suffered damages including, but not limited to: damages arising from identity theft and fraud; out-of-pocket expenses associated with procuring identity protection and restoration services; increased risk of future identity theft and fraud, and the costs associated therewith; and time spent monitoring, addressing, and correcting the current and future consequences of the Data Breach.

COUNT III
UNJUST ENRICHMENT
(On behalf of Plaintiff and All Class Members)

105. Plaintiff incorporates by reference and re-alleges each and every allegation set forth above in paragraphs 1 through 18 and paragraphs 24 through 62 as though fully set forth herein.

106. Plaintiff and Class Members conferred a benefit upon Defendant by using Defendant's services.

107. Defendant appreciated or had knowledge of the benefits conferred upon itself by Plaintiff. Defendant also benefited from the receipt of Plaintiff's and Class Members' Private Information, as this was used for Defendant to administer its services to Plaintiff and the Class.

108. Under principles of equity and good conscience, Defendant should not be permitted to retain the full value of Plaintiff and the Class Members' services and their Private Information because Defendant failed to adequately protect their Private Information. Plaintiff and the proposed Class would not have provided their Private Information to Defendant or utilized its services had they known Defendant would not adequately protect their Private Information.

109. Defendant should be compelled to disgorge into a common fund for the benefit of Plaintiff and Class Members all unlawful or inequitable proceeds received by it because of its misconduct and the Data Breach it caused.

COUNT IV
BREACH OF THE IMPLIED COVENANT OF GOOD FAITH AND FAIR DEALING
(On behalf of Plaintiff and All Class Members)

110. Plaintiff incorporates by reference and re-alleges each and every allegation set forth above in paragraphs 1 through 18 and paragraphs 24 through 62 as though fully set forth herein.

111. Defendant has violated the covenant of good faith and fair dealing by its conduct alleged herein.

112. Every contract in this state has an implied covenant of good faith and fair dealing. This implied covenant is an independent duty and may be breached even when there is no breach of a contract's actual and/or express terms.

113. Plaintiff and Class Members have complied with and performed all, or substantially all, of the obligations imposed by their conditions of services with Defendant.

114. Defendant breached the implied covenant of good faith and fair dealing by: failing to maintain adequate computer systems and data security practices to safeguard its patients' Private Information; failing to timely and accurately disclose the Data Breach to Plaintiff and Class Members; and continuing to accept and store Private Information and other personal information after Defendant knew, or should have known, of the security vulnerabilities of the systems that were exploited in the Data Breach.

115. Defendant acted in bad faith and/or with malicious motive in denying Plaintiff and Class Members the full benefit of their bargains as originally intended by the parties, thereby causing them substantial injury in an amount to be determined at trial.

COUNT V
INVASION OF CONFIDENCE
(On Behalf of Plaintiff and All Class Members)

116. Plaintiff incorporates by reference and re-alleges each and every allegation set forth above in paragraphs 1 through 18 and paragraphs 24 through 62 as though fully set forth herein.

117. At all times during Plaintiff's and Class Members' interactions with Defendant, Defendant was fully aware of the confidential and sensitive nature of Plaintiff's and Class Members' Private Information that Plaintiff and Class Members entrusted to Defendant.

118. As alleged herein and above, Defendant's relationship with Plaintiff and the Class was governed by terms and expectations that Plaintiff's and the Class Members' Private Information would be collected, stored, and protected in confidence, and would not be disclosed to unauthorized third parties.

119. Plaintiff and the Class entrusted Defendant with their Private Information with the explicit and implicit understandings that Defendant would protect and not permit the Private Information to be disseminated to any unauthorized third parties.

120. Plaintiff and the Class also entrusted Defendant with their Private Information with the explicit and implicit understandings that Defendant would take precautions to protect that Private Information from unauthorized disclosure.

121. Defendant voluntarily received Plaintiff's and Class Members' Private Information in confidence with the understanding that their Private Information would not be disclosed or disseminated to the public or any unauthorized third parties.

122. As a result of Defendant's failure to prevent and avoid the Data Breach from occurring, Plaintiff's and Class Members' Private Information was disclosed and misappropriated to unauthorized third parties beyond Plaintiff' and Class Members' confidence, and without their express permission.

123. As a direct and proximate cause of Defendant's actions and/or omissions, Plaintiff and the Class have suffered damages.

124. But for Defendant's disclosure of Plaintiff's and Class Members' Private Information in violation of the parties' understanding of confidence, their Private Information would not have been compromised, stolen, viewed, accessed, and used by unauthorized third parties. Defendant's Data Breach was the direct and legal cause of the theft of Plaintiff's and Class Members' Private Information as well as the resulting damages.

125. The injury and harm Plaintiff and the Class suffered was the reasonably foreseeable result of Defendant's unauthorized disclosure of Plaintiff's and Class Members' Private Information. Defendant knew or should have known its methods of accepting and securing Plaintiff's and Class Members' Private Information was inadequate as it relates to, at the very least, securing servers and other equipment containing Plaintiff's and Class Members' Private Information.

126. As a direct and proximate result of Defendant's breach of its confidence with Plaintiff and the Class, Plaintiff and the Class have suffered and will suffer injury, including but not limited to: (i) identity theft; (ii) the loss of the opportunity how their Private Information is used; (iii) the compromise, publication, and/or theft of their Private Information; (iv) out-of-pocket expenses associated with the prevention, detection, and recovery from identity theft, tax fraud, and/or unauthorized use of their Private Information; (v) lost opportunity costs associated with effort expended and the loss of productivity addressing and attempting to mitigate the actual

present and future consequences of the Data Breach, including but not limited to efforts spent researching how to prevent, detect, contest, and recover from tax fraud and identity theft; (vi) costs associated with placing freezes on credit reports; (vii) the continued risk to their Private Information, which remain in Defendant's possession and is subject to further unauthorized disclosures so long as Defendant fails to undertake appropriate and adequate measures to protect the Private Information of current and former patients; and (viii) present and future costs in terms of time, effort, and money that will be expended to prevent, detect, contest, and repair the impact of the Private Information compromised as a result of the Data Breach for the remainder of the lives of Plaintiff and Class Members.

127. As a direct and proximate result of Defendant's breaches of confidence, Plaintiff and the Class Members have suffered and will continue to suffer other forms of injury and/or harm, including, but not limited to, anxiety, emotional distress, loss of privacy, and other economic and non-economic losses.

PRAYER FOR RELIEF

WHEREFORE, Plaintiff, individually and on behalf of all others similarly situated, seeks judgment against Defendant, as follows:

(a) For an order determining that this action is properly brought as a class action and certifying Plaintiff as the representative of the Class and her counsel as Class Counsel;

(b) For an order declaring that Defendant's conduct violates the laws referenced herein;

(c) For an order finding in favor of Plaintiff and the Class on all counts asserted herein;

(d) For damages in amounts to be determined by the Court and/or jury;

(e) For an award of statutory damages or penalties to the extent available;

(f) For pre-judgment interest on all amounts awarded;

(g) For an order of restitution and all other forms of monetary relief; and

(h) Such other and further relief as the Court deems necessary and appropriate.

JURY TRIAL DEMANDED

Plaintiff demands a trial by jury of all claims in this Class Action Complaint so triable.

Dated: September 23, 2024

Respectfully submitted,

THE VAN WINKLE LAW FIRM

By: *s/ David M. Wilkerson*

David M. Wilkerson
NC State Bar No. 35742
11 North Market Street
(828) 258-2991
dwilkerson@vwlawfirm.com

Courtney E. Maccarone*
LEVI & KORSINSKY, LLP
33 Whitehall Street, 17th Floor
New York, NY 10004
Telephone: (212) 363-7500
Facsimile: (212) 363-7171
Email: cmaccarone@zlk.com

**pro hac vice* forthcoming

Counsel for Plaintiff